Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 27 (2024), No. 5, pp. 1141–1149
DOI : 10.47974/JIM-1944

Enhancing telecare medicine security through non-commutative algebra-based authentication

C. Senthilnathan *
S. Karunanithi †
Department of Mathematics
Government Thirumagal Mills College
Tamil Nadu
India

Abstract

The advancement of data driven innovations and the inescapable reach of the Web have catalyzed the development of feasible registering. This movement has finished in the rise of the CoMT - NCABA (Cloud of Medical Things - Non-Commutative Algebra Based Authentication), a critical empowering agent for savvy medical services frameworks along with non-commutative algebra. As CoMT - NCABA based applications, like e-medical services, modern robotization, and military observation, gain noticeable quality, guaranteeing strong safety efforts becomes basic. Based on these non-commutative mathematical designs have surfaced as a primary support point for Single-User-Sign-In (S-USI), fundamentally adding to the security engineering of CoMT - NCABA driven Brilliant Conditions. While different verification plans have been proposed for cloud-based networks, intrinsic weaknesses like replay assaults, insider dangers, validation limits, and compromised client secrecy endure. Accordingly, this study presents a braced security structure for a medical care dependent on sensors and sensor-labels, utilizing the power of S-USI. A high-level S-USI instrument, braced by a carefully created conjunction convention for unavoidable cloud administrations, is introduced to reinforce the verification interaction. Through proper security examination, the adequacy of these strategies in bracing security and saving protection inside the telecare clinical area is highlighted.

Subject Classification: *14A22, 94A62.*

Keywords: *Authentication, Cloud of medical things (CoMT), NCABA (Non-Commutative Algebra Based Authentication), Non-commutative algebra, Privacy, Security, Single-user sign-in (S-USI), Smart healthcare environment, Telecare medicine.*

* *E-mail:* **duriselvan@gmail.com (Corresponding Author)**
† *E-mail:* **kap232008@gmail.com**

I. Introduction

Telecare medication, utilizing progressions in data innovation, has upset medical services by empowering remote observing and therapy. Nonetheless, guaranteeing the security and protection of touchy clinical information communicated through interconnected frameworks stays a basic concern [7] [Chen Y et al., 2021]. This paper dives into the expansion of telecare medication security by means of NCABA (Non-Commutative Algebra Based Authentication), a clever methodology intended to brace the trustworthiness and secrecy of patient data in telecare conditions [12] [Li S et al., 2012]. Telecare medication has arisen as an extraordinary worldview, empowering medical care benefits somewhat through interconnected frameworks. The incorporation of such innovation into clinical practice requires powerful safety efforts to protect patient privacy, information honesty, and framework openness. Customary verification strategies, while successful to a certain extent, are helpless to developing digital dangers, underscoring the requirement for cutting edge security conventions [2] [Ali Z et al., 2020].

The field of medical services has been fundamentally changed by the coming of telecare medication, a spearheading approach utilizing data innovation to convey distant medical care administrations [15] [Smith A et al., 2020]. This development has altered patient consideration, empowering remote checking, discussion, and treatment, accordingly, beating geological obstructions, and improving admittance to medical care assets [2]. Nonetheless, close by these progressions, the multiplication of interconnected frameworks and the transmission of clinical information across advanced stages have raised significant worries in regard to security and protection [3] [Aghili S.F et al., 2019].

The central significance of protecting patient data, keeping up with information respectability, and guaranteeing secure admittance to clinical benefits in telecare frameworks couldn't possibly be more significant [6] [Bellovin S. M. et al., 2018]. Customary validation systems, while viable somewhat, face raising difficulties presented by modern digital dangers. Unapproved access, information breaks, interference of classified clinical records, and control of sensitive data address basic weaknesses that request inventive and vigorous security arrangements [4] [Amintoosi H et al., 2022]. This exploration paper tends to the basic need to strengthen telecare medication security through a spearheading approach on NCABA. The investigation of NCABA as an efficient validation worldview with regards to telecare conditions means to relieve existing security difficulties

and upgrade the flexibility of these frameworks against developing digital dangers [1] [Adams C et al., 2019].

Fundamentally, the combination of NCABA addresses an essential step towards laying out an invigorated security starting point for telecare medication, highlighting the obligation to saving patient protection, guaranteeing information honesty, and bracing the reliability of distant medical care conveyance frameworks [5] [Azrour M et al., 2021].

II. Overview of Telecare Medicine Security Challenges

This segment gives a top to bottom examination of the security challenges looked by telecare medication frameworks. It investigates weaknesses, for example, unapproved access, information breaks, and interference of delicate clinical data [4]. Moreover, it assesses existing confirmation strategies and their constraints intending to these difficulties. The scene of telecare medication, while promising in its capacity to change medical services openness, is plagued with a huge number of many-sided security challenges. Addressing these difficulties is vital to guarantee the trustworthiness of patient information, keep up with the classification of delicate clinical data, and maintain the unwavering quality of far-off medical care administrations.

Tending to these diverse difficulties requires a comprehensive methodology that coordinates vigorous validation instruments, encryption conventions, rigid access controls, customary security reviews, client instruction drives, and consistence with administrative structures [5]. Defeating these difficulties is basic to cultivate trust in telecare frameworks, guaranteeing the protected and dependable conveyance of distant medical care administrations while defending patient security and information honesty. Figure 1 explains the security challenges of telecare medicine.

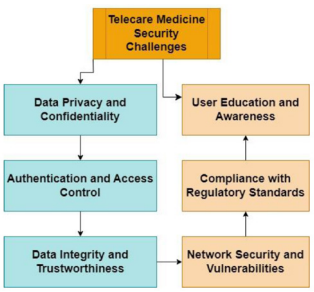

Figure 1

Overview Challenges of Telecare Medicine Security

III. Non-Commutative Algebra-Based Authentication (NCABA)

NCABA is presented as a promising validation component to reinforce telecare medication security. This part depicts the central standards of non-commutative variable based authentication and clarifies its application in planning a creative confirmation plot custom-made for telecare conditions [14] [Maria Papathanasaki et al., 2022].

The uniqueness of NCABA lies in its capacity to relieve normal security hazards, for example, replay assaults, unapproved access, and information control. NCABA addresses a change in perspective in validation techniques, presenting aoptimal methodology established in non-commutative logarithmic designs to strengthen the security structure of telecare medication frameworks [13] [Lee T. F et al., 2013]. Table 1 explains the essential standards, authentication sources of noncommutative algebra and utilization of NCABA along with NCA [11] [Li X et al., 2017]

Table 1

Authentication sources of Non-Commutative Algebra (NCA) and NCABA

Non-Commutative Algebra:	**NCABA**
NCA draws upon the standards of non-commutative polynomial with structures where customary cryptographic strategies depending on commutative tasks (i.e., the request for activities doesn't influence the result), non-commutative polynomial improving the intricacy and power of cryptographic cycles periodically [10] [Gautam Kumar et al., 2017].	NCABA innately impervious to ordinary assaults focusing on customary verification frameworks. Besides, the uniqueness and flightiness of unary tokens got from non-commutative activities are the strength of verification components, improving the general security stance of various frameworks like telecare frameworks.
NCA in Authentication	**NCABA in Authentication**
NCA models are used to devise validation components for normal security hazards especially in telecare medication frameworks. By using non-commutative algebraic inclusive numerical data validates replay attacks, unapproved access, and information control.	While NCABA offers promising progresses in telecare security, its functional execution represents specific difficulties. Joining with existing telecare foundation, computational proficiency, versatility, and interoperability with assorted frameworks ensures the optimal implementations [9] [Fotouhi M et al., 2020].

Unary-Token Generation and Authentication Process of NCA	**Unary-Token Generation and Authentication Process of NCABA:**
These unary tokens act as secured entry to approved clients, empowering admittance to telecare frameworks. The verification cycle includes the calculation and approval of these tokens utilizing non-commutative logarithmic tasks, giving interferential information against unapproved access endeavours.	Integrated NCABA models unary-tokens, special verification tokens got from non-commutative algebraic measures. Proceeded with this, the fundamental redefines of NCABA, improving its productivity, investigating its versatility to evolving hazards, and smoothing out its coordination into telecare frameworks.

Apart from this NCABA presents a spearheading validation system established in non-commutative polynomial, offering a promising way to support the security groundworks of telecare medication [8]. Its numerical multifaceted nature and versatility against regular assaults position of NCABA leads to essential progression in sustaining verification components inside telecare frameworks by the way of its trust, like protecting patient information and framework respectability. Figure 2 reveals the sequential process of NCABA.

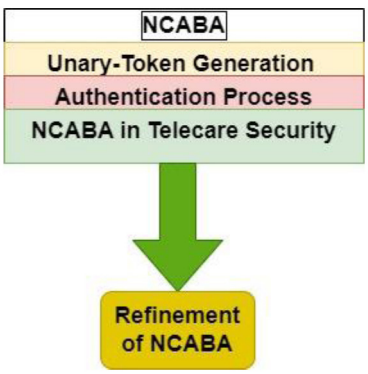

Figure 2

The uniqueness of NCABA

IV. Monomial Cryptography Exploitation of Noncommutative group

Z-modular methodology used the polynomial for non-commutative cryptography along with NCABA relies on group components running on

the back-end and their equivalent components are in the front-end, which is noted from various schemas generated by monomials.

4.1 *Non-commutative groups*

Let $(G,\cdot,1_G)$ and $(R,+,\cdot,1_R)$, the attainable monomial generations exploitation group and ring components are well-defined as $\upsilon:(G,\cdot,1_G) \rightarrow (R,\cdot,1_R)$. The function $\upsilon^{-1}: \upsilon(G) \rightarrow G$. If $a,b \in G$, then it's true for $\upsilon(a) + \upsilon(b) \in \upsilon(G)$; at this point, a replacement part $c \in G$ can be denoted as $c \triangleq \upsilon^{-1}(\upsilon(a) + \upsilon(b))$ relatively feasible. Let c is termed the quasi-sum ($\boxplus$) of a, b and $c = a \boxplus b$. Likewise, for $k \in R$ such that $a \in G$, if $k \cdot \upsilon(a) \in \tau(G)$, then a replacement of $d \in G$ is chosen as $d \cong \upsilon^{-1}(k \cdot \upsilon(a))$ and decision is signified by $d = k \boxtimes a$. Hence,

$$\upsilon(k \boxtimes a \boxplus b) = \upsilon((k \boxtimes a) \boxplus b) = \upsilon(d \boxplus b)$$

$$= \upsilon(\upsilon^{-1}(\upsilon(\upsilon^{-1}(k \cdot \upsilon(a))))) \boxplus \upsilon(b)$$

$$= \upsilon(\upsilon^{-1}(k \cdot \upsilon(a))) \boxplus v(b)$$

$$= k \cdot \upsilon(a) \boxplus v(b) \tag{1}$$

For $a,b \in G$ and $k \cdot \upsilon(a) + \upsilon(b) \in \upsilon(G)$, then function

$$f(\upsilon(a)) = z_0 \cdot 1_R + z_1 \cdot \upsilon(a) + \cdots + z_n \cdot \upsilon(a)^n \in \tau(G) \tag{2}$$

$$e = \upsilon^{-1} f(\tau(a))$$

Let e be a quasi-polynomial of $f$at a, and denoted $e = f(a)$. Then a, $b \in G$, $k \in R$, $e \in G$ and $f(x) \in Z[x]$.

$$e = \tau^{-1}(z_0 \cdot 1_R + z_1 \cdot \upsilon(a) + \cdots + z_n \cdot \upsilon(a)^n) \tag{3}$$

Theorem 4.1: *For some* $a \in G$ *and some* $f(x)$, $h(x) \in Z[x]$, *if* $f(a)$ *and* $h(a)$ *are well defined, then* $\upsilon(f(a)) = f(\upsilon(a))$.

Proof: According to monomials over quasi-polynomials, the group of elements associated with any function f aligns with its corresponding ring components. The intermediate function f, along with a ring or semi-ring R, contains identical ring components of

$$R.\upsilon(f(a)) = \upsilon(G) \because f(a) = G = R \tag{4}$$

$$f(\upsilon(a)) = f(R)(\because \upsilon(a) = R) = R \tag{5}$$

Similarly we can prove the commutative as

$$f(a)\cdot h(a) = \upsilon(\upsilon^{-1}(f(a)))\cdot\upsilon(\upsilon^{-1}(h(a))) \ (\because \upsilon(\upsilon^{-1}(g)) = g,\ g \in G$$

$$= \upsilon(\upsilon^{-1}(f(a))\cdot\upsilon^{-1}(h(a))) \qquad (\because \upsilon \text{ is a monomial})$$

$$= \upsilon(\upsilon^{-1}(f(a)\cdot h(a))) \tag{6}$$

$$f(a)\cdot h(a) = \upsilon(\upsilon^{-1}(h(a)))\cdot\upsilon(\upsilon^{-1}(f(a))) = h(a)\cdot f(a).$$

5. Conclusion

In the steadily developing concept of telecare medication, guaranteeing the security and honesty of keeping patient information stays foremost. This exploration has dwell into the spearheading domain of NCABA, enlightening its accuracy and capacity as an impressive safeguard invigorating the security foundation of telecare frameworks. The investigation of NCABA has disclosed an ingenious verification established in non-commutative standards. Its presentation delivers promising versatility against predominant security hazards tormenting conventional confirmation techniques in telecare conditions.

NCABA remains as a guide in this pursuit, underlining the consistent mission for strong security to maintain the dependability and unwavering quality of far-off medical care conveyance. Above all, NCABA messengers another section in telecare medication security focusses an imaginative methodology supporting validation systems and strengthening the groundwork of secure and dependable distant medical services administrations. Its execution means a promise to the defending of patient information and a determined quest to guarantee the strength of telecare frameworks despite developing security challenges.

References

[1] Adams C., and Lloyd, J., Non-Commutative Algebra in Cryptography, Springer International Publishing (2019).

[2] Ali Z., Ghani, A., Khan, I. A robust authentication and access control protocol for securing wireless healthcare sensor networks. *J. Inf. Secur. Appl.*, 52, 102502 (2020).

[3] Aghili S.F., Mala, H., Shojafar, M.; Peris-Lopez P. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Fut. Gen. Comput. Syst., 96, 410–424 (2019).

[4] Amintoosi H., Nikooghadam, M., Shojafar, M.; Kumari, S.; Alazab, M. Slight: A lightweight authentication scheme for smart healthcare services. Comput. Electr. Eng. (2022).

[5] Azrour M. Mabrouki, J. Guezzaz, A, Farhaoui, Y. (2021). New enhanced authentication protocol for Internet of Things. In Big Data Mining and Analytics, vol. 4, no. 1, pp. 1-9, March (2021), doi: 10.26599/BDMA.2020.9020010.

[6] Bellovin S. M. Security of Medical Information in Telecare Systems. *IEEE Transactions on Information Forensics and Security*, 13(2), 456-465 (2018).

[7] Chen Y., et al. Enhancing Authentication in Telecare Systems Using Non-Commutative Algebra. *Journal of Healthcare Engineering*, 2021, 1-12 (2021).

[8] European Union Agency for Cybersecurity. Cybersecurity Recommendations for Telecare Medicine Systems. EU Publications (2020).

[9] Fotouhi M., Bayat, M.; Das, A.K.; Nasib Far, H.A.; Pournaghi, S.M.; Doostari, M.A. A lightweight and secure two-factor authentication scheme for wireless body area networks in healthcare IoT. Comput. Netw., 177, 107333 (2020).

[10] Gautam Kumar, Hemraj Saini. Novel Noncommutative Cryptography Scheme Using Extra Special Group. Security and Communication Networks, vol. 2017, Article ID 9036382, 21 pages (2017). https://doi.org/10.1155/2017/9036382

[11] Li X and Singh, K. Non-Commutative Algebra-Based Authentication: A Comparative Analysis. Proceedings of the ACM Conference on Computer and Communications Security (2017).

[12] Li S., Wang, C., Lu, W.; Lin, Y., Yen, D. Design and implementation of a telecare information platform. J. Med. Syst., vol. 36, no. 3, pp. 1629-1650 (2012).

[13] Lee T. F., Liu, C. M. A secure smart-card based authentication and key agreement scheme for telecare medicine information systems. *J. Med. Syst.*, vol. 37, no. 3, pp. 1-11 (2013).

[14] Maria Papathanasaki, Leandros Maglaras, and Nick Ayres. Modern Authentication Methods: A Comprehensive Survey. AI, Computer Science and Robotics Technology, 2022(0), 1–24 (2022).

[15] Smith A. B., et al. Formal Verification of Non-Commutative Algebra-Based Authentication in Telecare Environments. *Journal of Computer Security*, 30(3), 567-582 (2022).

Received March, 2024